Premières considérations sur les questions de responsabilité liées aux paiements par WAP

Montero, Etienne

Published in:
Transferts électroniques de fonds

Publication date:
2001

Document Version
le PDF de l'éditeur

PREMIÈRES CONSIDÉRATIONS SUR LES QUESTIONS DE RESPONSABILITÉ LIÉES AUX PAIEMENTS PAR WAP

PAR

Etienne MONTERO (*)

PROFESSEUR AUX FACULTÉS UNIVERSITAIRES NOTRE-DAME DE LA PAIX À NAMUR

(*) J'adresse mes plus vifs remerciements à Jean-Pierre VANDELOISE (Banksys) pour ses précieuses explications techniques et pour m'avoir si aimablement autorisé à reproduire certains schémas ayant servi de support à son intervention au colloque du 5 octobre dernier. Je tiens à remercier aussi chaleureusement Laetitia ROLIN JACQUEMYNS pour sa collaboration efficace sous diverses formes.

Introduction

Le juriste est habitué à entendre le petit couplet stigmatisant le retard du droit par rapport aux évolutions technologiques. Il n'en était que plus tentant de répondre présent à l'appel des organisateurs du colloque sur « les aspects juridiques des paiements par WAP », qui s'est tenu à Bruxelles le 5 octobre 2000. Cette fois, à coup sûr, des juristes allaient être, sinon en avance, en tout cas pas en retard, dès lors que cette nouvelle technologie en est à ses premiers balbutiements et n'a pas encore suscité le moindre contentieux.

Certes il n'y a pas de jurisprudence (1) pour nourrir la réflexion, ni étude doctrinale spécifique. L'exercice n'en est que plus stimulant. Néanmoins il saute aux yeux que le paiement par WAP n'est qu'une variété de télépaiement, qui, lui, a déjà fait l'objet de plusieurs études juridiques. Il est donc permis de penser, *a priori*, qu'usage peut être fait du raisonnement par analogie.

Cette dernière observation conduit à s'interroger sur la pertinence du sujet retenu. N'est-on pas précisément en droit de penser que le paiement par WAP, loin de présenter la moindre nouveauté sur le plan juridique, se réduit à une forme de télé-

(1) Toutefois, en jurisprudence française, une première décision a été rendue et publiée récemment (Com. Paris, ord. réf., 30 mai 2000, *Dalloz*, n° 30, 2000, p. 349), et confirmée en appel en juillet 2000. En l'espèce, il était reproché à France télécom de fausser la concurrence et d'abuser de sa position dominante dans le secteur de la fourniture d'accès à internet au moyen du téléphone mobile ainsi que sur le marché du portail donnant accès à l'internet mobile et aux services connexes, et ce, dans la mesure où les téléphones « waplockés » vendus par ses filiales comportent comme page d'accueil internet celle correspondant au fournisseur d'accès « i itinéris » de France télécom, voie de passage obligée pour avoir accès aux services fournis par d'autres fournisseurs d'accès. Estimant la demande fondée (au moins partiellement), le juge des référés fait interdiction, sous astreinte, à France télécom et à ses filiales de continuer à commercialiser des téléphones mobiles qui, d'une part, n'indiqueraient pas clairement la préprogrammation du numéro du fournisseur d'accès à internet de France télécom et, d'autre part, ne comporteraient pas la possibilité, clairement indiquée, de remplacer ce numéro par celui d'un autre fournisseur d'accès internet selon le vœu de l'utilisateur et moyennant quelques manœuvres simples.

paiement et obéit dès lors à un régime juridique d'ores et déjà largement maîtrisé et commenté (2) ?

Intuitivement, on devine certes qu'il n'est pas question d'une révolution dans la pratique et le droit des moyens de paiement. En même temps, l'histoire enseigne que l'essor du commerce, sous ses diverses formes, a toujours été accompagné par de nouveaux développements de la monnaie et des moyens de paiement. A chaque forme nouvelle de commerce correspond une catégorie particulière et originale de moyen de paiement (3).

Le commerce de proximité, tel que pratiqué dans les sociétés traditionnelles, se satisfait globalement de l'utilisation de la monnaie fiduciaire. Toutefois, étant un titre non dématérialisé et au porteur, ce type de monnaie reste limité à l'acquittement de faibles dépenses, pour des raisons évidentes de sécurité physique. En outre, la monnaie fiduciaire est inutilisable aussi bien pour des paiements nécessitant la mise en œuvre d'un mécanisme de crédit que pour des paiements à distance. Le commerce moderne ne pouvait s'accommoder de pareille forme de monnaie. Aussi la pratique a-t-elle innové en imaginant les effets de commerce et le chèque, et plus récemment, le virement et le paiement par carte. Plus tard, pour faire face aux risques et besoins propres au commerce international, d'autres mécanismes juridiques ont vu le jour, tel le crédit documentaire.

L'avènement du commerce électronique (*e-commerce*) a supposé, lui aussi, l'apparition de nouveaux modes de paiement : l'*e-banking* (le *home banking* et l'*internet ou web banking*), le télépaiement, les diverses formes de « monnaie électronique » ou « virtuelle », le recours à des intermédiaires non bancaires... L'*e-commerce* aurait eu peu de chance de prospérer si l'ordre de paiement n'avait pu être émis directement sur l'internet, le

(2) Par exemple, M. Vivant, C. Le Stanc et alii, *Lamy droit de l'informatique et des réseaux*, éd. 2000, n^os^ 2724 et s.; E. Caprioli, « Le régime juridique des paiements sur internet », in *Internet saisi par le droit, Travaux de l'A.F.D.I.T.* sous la direction de X. Linant de Bellefonds, Paris, Éd. des Parques, 1997, pp. 61-94; E. Wymeersch, « Aspects juridiques de certains nouveaux moyens de paiement », *Revue de la Banque*, 1/1995, pp. 17-39; J. Huet, « Aspects juridiques du télépaiement », *J.C.P.*, G, 1991, I, 3524, pp. 287 et s.; et les autres études citées *infra*.

(3) Lire M. Espagnon, « Le paiement d'une somme d'argent sur internet : évolution ou révolution du droit des moyens de paiement ? », *J.C.P.*, G, 1999, I 131, pp. 787 et s.

commerçant souhaitant naturellement recevoir l'ordre et la commande en ligne simultanément. Enfin, l'apparition des GSM WAP devrait favoriser, dans les prochaines années, l'émergence d'une nouvelle forme de commerce, le *m-commerce*. Dans la perspective historique suggérée à grands traits, il apparaît légitime et pertinent de se demander si, du point de vue des paiements, le commerce mobile représente une nouvelle étape ou, au contraire, se développera sans solution de continuité avec l'*e-commerce*.

Le propos — limité — de la présente étude, est de commenter quelques questions de responsabilité liées au paiement par WAP. Bien d'autres questions seront passées sous silence dans la mesure où elles ont été confiées à d'autres rapporteurs, en particulier celles relatives à la preuve ou celles ressortissant au droit de la consommation (p.ex., l'articulation entre le caractère irrévocable de l'ordre de paiement et l'exercice du droit de rétractation reconnu en matière de contrats conclus à distance).

Il reste à préciser que la notion de paiement est entendue ici, non au sens large du droit des obligations, mais au sens, plus étroit, du langage courant. Quoique le paiement figure, dans le Code civil, parmi les modes d'*extinction* des obligations (art. 1234), une doctrine autorisée préfère y voir, à juste titre, avant tout, l'*exécution* normale de l'obligation; l'extinction de l'obligation à l'égard du créancier payé apparaît en réalité comme la conséquence logique de cette caractéristique première (4). Dans cette perspective, le paiement a pu être défini comme l'exécution volontaire, en nature, de l'obligation telle qu'elle est née initialement, quelle qu'en soit la source (5). Cela étant, dans cette contribution, la notion de paiement est comprise, dans un sens plus étroit, comme l'acquittement d'une dette portant sur une somme d'argent. On s'intéresse au paiement seulement en tant qu'il a pour objet de la monnaie, sous quelque forme que ce soit.

(4) P. Van Ommeslaghe, « Le paiement. Rapport introductif », Actes du colloque « Les aspects juridiques du paiement » des 3 et 4 décembre 1992, *Rev. Dr. ULB*, n° 8, 1993, p. 10.

(5) *Ibidem*.

DESCRIPTION DES PRINCIPAUX MODES DE PAIEMENT PAR WAP

D'un point de vue technique, le WAP est une première tentative pour ouvrir le monde de l'internet aux utilisateurs de téléphones portables. « WAP sont les initiales de *'Wireless Application Protocol'* (Protocole d'Application Mobile). Au départ, ce protocole a été créé à l'initiative d'entreprises comme Nokia ou Ericsson. Il est basé sur des technologies Internet existantes comme le XML et IP » (6).

Il semble que le WAP ne soit que la première étape d'une longue évolution. Son principal défaut est de n'offrir qu'un débit limité à 9.6 Kbit/s, ce qui est loin du débit moyen d'un modem actuel. D'autres protocoles très attendus devraient pallier cette carence, comme par exemple le HSCSD (High Speed Circuit Switched Data) et le GPRS (General Packet Radio Service). Il est également beaucoup question dans la presse de l'UMTS (Universal Mobile Telecommunication System), dont les licences viennent d'être attribuées dans certains pays européens et qui devrait permettre un débit d'environ 2 Mbit/s. Si seul le WAP est commercialisé pour le moment, il est, de toute évidence, une technologie de transition. Tout porte à croire que le WAP est aux systèmes de communications mobiles de la troisième génération ce qu'est le Minitel à l'internet. Un banc d'essai en quelque sorte...

Du point de vue commercial, le WAP doit être considéré comme un nouveau canal de distribution qui n'est pas fondamentalement différent de l'internet, si ce n'est qu'il offre une plus grande mobilité aux « waponautes » qui peuvent réaliser des transactions d'ordres divers *via* leur téléphone portable. La question qui se pose immédiatement est la suivante : comment effectuer un paiement par le WAP ? Il semble clair que la plupart des moyens de paiement utilisables sur l'internet pourraient théoriquement être étendus, moyennant quelques adaptations techniques, au WAP. On songe ainsi à la carte de

(6) Pour plus d'informations sur le WAP, voy. ite http://www.sowap.com/wap-faq.html

crédit, à l'instrument rechargeable de type Proton (7), au virement électronique, aux jetons monétaires électroniques (souvent qualifiés par la presse et le grand public de « monnaie électronique »), ou encore au recours à des intermédiaires non bancaires pour effectuer le paiement (8).

Un examen plus attentif de la question montre rapidement que certains moyens de paiement sont beaucoup moins adaptés que d'autres au WAP. On peut d'emblée écarter les jetons monétaires électroniques qui sont peu répandus dans le monde et absents de la panoplie des moyens de paiement offerts au public belge. Les intermédiaires non bancaires, quant à eux, s'ils ont défrayé la chronique dans les années 1994 à 1997, n'ont jamais vraiment réussi à s'imposer (9).

En Belgique, les solutions de paiement sérieusement envisagées dans le cadre du WAP sont dès lors les cartes de crédit, l'instrument rechargeable et le virement électronique.

A. – *M-Commerce*

La première application envisagée repose sur l'utilisation de la carte de crédit, qui est sans doute l'instrument de paiement le plus répandu sur l'internet. Les systèmes proposés ont souvent le grand défaut de ne pas offrir une sécurité suffisante dans le transfert du numéro de la carte.

Banksys, en collaboration avec les principales banques du pays, travaille actuellement à une utilisation de la carte de crédit, comme mode de paiement par WAP adapté au *m-commerce*, fondée sur un système d'application bancaire et d'outils de cryptage intégrés dans le terminal GSM sur la carte SIM. Ce système devrait permettre une communication hautement

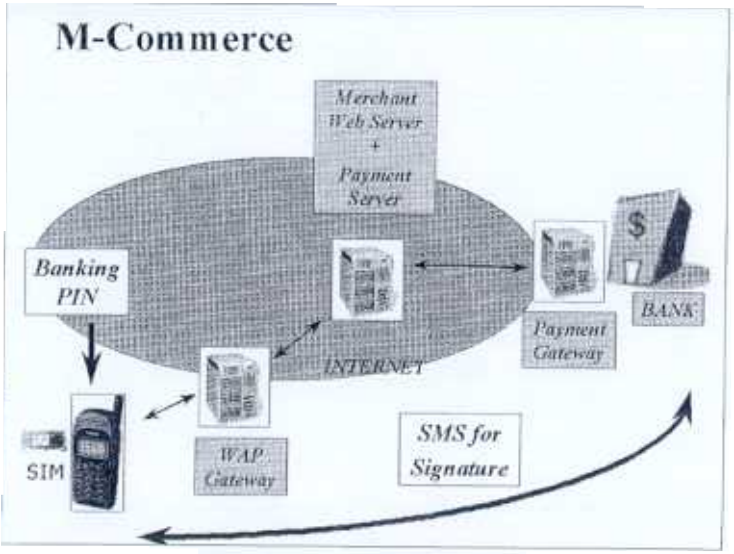
(7) A ce sujet, F. MOURLON BEERNAERT, « Les cartes à mémoire pré-payées (pre-paid cards) : un nouvel instrument de paiement », *J.T.*, 1997, pp. 377-385.

(8) Sur ces deux derniers systèmes de paiement, voy., en particulier, E. CAPRIOLI, « Le régime juridique des paiements sur internet », *op. cit.*, pp. 61 et s., spéc. pp. 69-71 ; J.-P. BUYLE et O. POELMANS, « Description des moyens de paiement en réseau ouvert », in E. MONTERO (éd.), *Internet face au droit, Cahiers du CRID*, n° 12, E. Story-Scientia, 1997, pp. 87-109 ; V. SÉDALLIAN, *Droit de l'internet*, Coll. et éd. AUI, 1996, spéc. pp. 221-232.

(9) Pour plus d'informations, voy. L. ROLIN JACQUEMYNS, « Comment payer par Internet aujourd'hui ? Le choix du système adéquat », *Revue Ubiquité*, 2000/7, pp. 91-97.

sécurisée du numéro de la carte de crédit. La procédure peut être décrite brièvement comme suit.

A l'aide de son GSM WAP, un utilisateur se connecte à un site WAP pour y passer commande d'un bien. Après avoir effectué son choix, il transmet sa commande ainsi que son accord pour payer au commerçant. Ce dernier s'adresse à la banque de l'utilisateur, laquelle envoie un SMS sur le GSM de celui-ci indiquant la commande et le montant à payer. Pour confirmer la transaction, l'utilisateur introduit son code confidentiel (B-PIN), ce qui active le mécanisme de signature de la commande; le résultat est mis dans un SMS qui est expédié vers la banque, laquelle, après vérification opérée par Banksys (de la validité de la carte de crédit, du disponible sur la carte...), exécute le paiement.



© Jean-Pierre Vandeloise, Banksys

Dans d'autres pays, une solution alternative a été développée, qui repose sur l'utilisation d'une carte de crédit dotée d'une puce. Dans la vie courante, l'ordre de paiement est donné par le client qui saisit son code confidentiel sur un terminal spécifique (un terminal point de vente chez un commerçant, par exemple). Pour transposer ce système au GSM, il faut un lecteur *ad hoc* intégré dans le portable WAP.

Ainsi, la France a mis au point une application bancaire intégrée dans la carte bleue. Celle-ci serait lue par le portable WAP doté de la technologie connue sous le nom de « dual slot », une sorte de fente placée sur le côté de l'appareil qui permet l'insertion de la carte. Le fait d'introduire le code confidentiel pour valider la transaction déclenche l'opération de signature (identification des parties) et permet une transmission chiffrée.

B. — *M-Banking*

Ces dernières années ont vu la multiplication des services de banque à distance. On a connu successivement la banque par téléphone (*phone banking*), la banque à domicile (*home banking*) par le biais d'une liaison point à point, la banque par l'internet (*net* ou *web banking*). Aussi est-il tout naturel que le WAP ait aussi son application bancaire, en l'occurrence, le *m-banking*. En Belgique, l'une ou l'autre banques (Dexia, KBC...) disposent déjà d'un site WAP permettant de réaliser des opérations de *m-banking*.

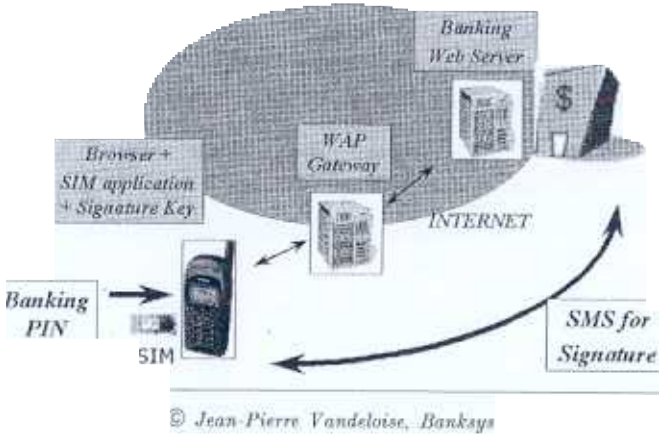
Toutes ces applications ne sont que diverses formes de télévirement et fonctionnent selon un schéma comparable : au moyen d'un terminal connecté au réseau bancaire, le débiteur donne un ordre de virement à une banque auprès de laquelle il a un compte. Ce moyen de paiement n'est pas parfaitement adapté au commerce électronique car, ici, l'ordre de paiement est reçu non par le commerçant, mais par l'établissement de crédit. Certaines banques ont cependant envisagé de faire profiter les commerçants de ces systèmes en leur permettant d'envoyer au client qui réalise des achats sur leur site un virement électronique, ce qui lui permet d'effectuer le paiement *via* le système sécurisé offert par la banque (10).

Dans le cas du WAP, le procédé serait le suivant. A l'aide de son GSM WAP, l'utilisateur arrive sur le site WAP de la banque, à laquelle il donne l'ordre d'effectuer un versement de autant au profit de tel créancier. La banque sollicitée envoie

(10) C'est le cas, par exemple, du système *Home Pay* mis en place par la BBL.

un SMS sur le GSM du donneur d'ordre indiquant la commande et le montant à payer. Pour confirmer la transaction, l'utilisateur introduit son code confidentiel (B-PIN), qui active le mécanisme de signature de la commande et met le résultat dans un SMS qui est aussitôt expédié vers la banque, laquelle, après les vérifications d'usage, exécute le paiement.

M-Banking

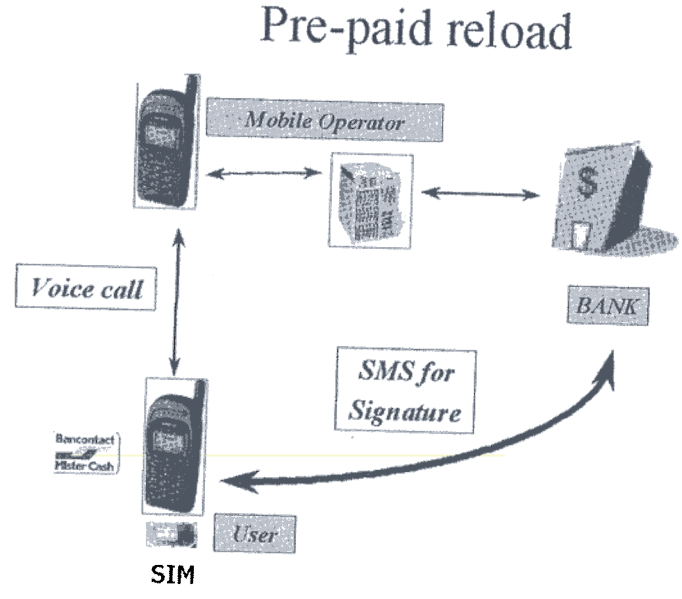


C. — *Systèmes de paiement basés sur la notion d'« argent électronique »*

Une troisième solution intéressante pourrait être basée sur l'utilisation d'un instrument rechargeable matérialisé dans un carte prépayée (et, le cas échéant, multiprestataire).

Ce « porte-monnaie électronique » permet d'émettre un ordre de paiement sur un réseau selon le schéma du paiement par carte, mais s'en distingue d'un double point de vue : d'une part, son utilisation est liée à un prépaiement, d'autre part, il a vocation à traiter uniquement des ordres portant sur de petits montants. Pour pouvoir utiliser un instrument rechargeable pour les paiements en ligne, il est nécessaire que l'utilisateur dispose d'un lecteur intégré à son GSM WAP.

Préalablement à toute utilisation de la carte, son titulaire doit charger un montant monétaire sur lequel viendront s'imputer les paiements (à l'opérateur, dans le schéma ci-dessous). Les données électroniques correspondant au solde disponible prépayé figurent sur le microcircuit de la carte ou éventuellement sur la mémoire de l'ordinateur de l'organisme dépositaire du montant (11). Le processus de paiement et de signature est similaire à ceux que nous avons mentionnés dans le cas du *m-commerce* et du *m-banking*.



Ce type d'instrument de paiement présente cependant une particularité, qui réside dans la séparation entre le processus d'authentification, qui n'a pas lieu en ligne puisque l'instrument a été chargé préalablement *via* un contact direct avec la

(11) Dans ce cas, on parlera plutôt de « porte-monnaie virtuel »

banque (comme c'est le cas avec la carte Proton), et la communication entre les partenaires à la transaction. De ce point de vue, on peut considérer que la sécurité est bien assurée. Il reste à se demander ce qu'il advient du montant chargé sur cet instrument en cas de perte ou de vol du GSM ? Le système qui prévaut en Belgique pour les instruments rechargeables est que la perte de l'instrument chargé équivaut à la perte d'une somme de monnaie fiduciaire équivalente et de la carte qui vaut quelques centaines de francs. Dans le cas du WAP, le titulaire de l'instrument perd non seulement sa carte, mais également son terminal GSM.

II. Le cadre juridique du paiement par WAP

Dès l'instant où il se trouve déclenché par le biais d'une carte, le paiement par WAP, à l'instar des autres formes de télépaiement, a vocation à être gouverné par les règles applicables au paiement par carte.

En France, cette analyse s'impose naturellement puisque c'est, physiquement, la carte à puce (la fameuse « carte bleue ») elle-même qui va servir à déclencher l'ordre de paiement. La seule nouveauté par rapport au paiement par carte traditionnel réside dans le type de terminal utilisé. Celui-ci n'est pas l'usuel terminal point de vente (TPV), mais le GSM WAP muni d'un lecteur de carte à puce.

Dans la solution de type *e-commerce*, préconisée en Belgique par Banksys, l'analyse est un peu différente, mais permet également de conclure à un paiement par carte. Voyons cela de plus près, en reprenant, pas à pas, le mécanisme de paiement mis au point. Une carte de crédit (ou plusieurs) est raccrochée à la clé privée (qui permet de signer) contenue dans la carte SIM intégrée au GSM. Comme on l'a expliqué précédemment, le client adresse une requête à une « passerelle » (WAP Gateway), qui dirige celle-ci vers le serveur où se trouve hébergé le site WAP recherché. Le client passe commande et marque son accord sur un montant à payer (le numéro de la carte de crédit ne transite jamais par le réseau). Le commerçant sollicité s'adresse alors à la banque, qui envoie un SMS sur le portable

du client pour confirmation de la commande et de l'ordre de paiement et pour signature. Si plusieurs cartes de crédit ont été liées à la signature, le client choisit celle qu'il souhaite utiliser. Pour confirmer la transaction, il introduit son code secret (ou *Banking-Pin* (12)) : dès lors l'application bancaire logée dans la carte SIM active la clé privée de manière à mettre en œuvre le mécanisme de signature. Le résultat de l'opération est recueilli dans un SMS et expédié vers la banque. Avant d'exécuter l'ordre de paiement, cette dernière se tourne vers Banksys qui, après les vérifications usuelles, donne l'autorisation d'accepter l'ordre de paiement (et envoie au CEC l'ordre de débiter le compte du client au profit du commerçant). Il se pourrait qu'en matière de cartes VISA, cette étape s'opère au niveau d'un serveur propre à VISA.

C'est le certificat contenant la clé publique (complémentaire à la clé privée) qui fait le lien entre la clé privée et la carte de crédit (il n'y a pas d'information concernant la carte de crédit dans la carte SIM). Un tel certificat comprend 1° la clé publique, 2° des informations relatives à la carte de crédit, 3° le sceau de l'autorité de certification. Le *lien* entre la clé privée (signature) et la carte de crédit est *réalisé concrètement au niveau de Banksys* qui gère le répertoire contenant les certificats de clés publiques. Enfin, il est à noter que l'opération sera portée sur le relevé mensuel du porteur de la carte, ce qui signifie concrètement qu'elle figurera au titre des opérations réalisées au moyen de sa carte de crédit.

Au total, ce schéma s'apparente fortement à celui mis en œuvre en matière de paiement par carte de crédit à l'aide de terminaux points de vente (TPV). Tout le système de protection mis en place soit par VISA, soit par Mister Cash va trouver à s'appliquer. Cette présentation a une incidence en matière d'opposition en cas de perte/vol de la carte, comme on le verra (*infra*, III, A).

12) Personal Identification Numbe

Il est à noter qu'un paiement par carte est assimilable à un ordre de virement (13), auquel fait suite un transfert électronique de fonds, soit une opération consistant, par un jeu d'écritures, à débiter un compte d'une somme déterminée afin de la porter au crédit d'un autre compte en banque.

Le *m-banking*, lui, consiste en des ordres de paiement que le client adresse à sa banque, soit des « virements électroniques » auxquels s'appliquent les règles traditionnelles du virement (14). En pratique, il est régi fondamentalement par les conditions contractuelles entre la banque et son client. Le dispositif de protection mis en place dans le cadre de l'utilisation des cartes de crédit ne trouve pas à s'appliquer.

Les règles *spécifiques* applicables au paiement par carte sont peu nombreuses (15). Mais il en est quelques unes, issues de la jurisprudence des cours et tribunaux et des avis de l'Ombudsman...

Il y a aussi et surtout la Recommandation de la Commission européenne du 30 juillet 1997 « concernant les opérations effectuées au moyen d'instruments de paiement électronique, en particulier la relation entre émetteur et titulaire » (16). Cette recommandation, bien que dépourvue de caractère obligatoire, est généralement suivie dans les conditions générales des contrats proposés par les banques pour la mise à disposition des cartes de crédit, d'autant que si sa mise en œuvre devait être jugée insatisfaisante la Commission européenne proposerait une « législation contraignante appropriée » (préambule, considérant n° 12).

(13) En ce sens, X. THUNIS, *Responsabilité du banquier et automatisation des paiements*, Namur, P.U.N., 1996, pp. 86 et s.; X. THUNIS et M. SCHAUSS, « Aspects juridiques du paiement par carte », *Cahiers du CRID*, n° 1, E. Story-Scientia, 1988, spéc. pp. 17-18; J.-P. BUYLE, « La carte de paiement électronique », in *La banque dans la vie quotidienne*, Bruxelles, Éditions du Jeune Barreau, 1986, p. 458; P. VAN OMMESLAGHE, *op. cit.*, p. 28; M. VASSEUR, « Le paiement électronique. Aspects juridiques », *J.C.P.*, 1985, I, 3206, spéc. n° 7.

(14) Sur le régime juridique du virement, voy. X. THUNIS, *op. cit.*, pp. 93 et s.; A. BRUYNEEL, « Le virement », in *La banque dans la vie quotidienne*, Bruxelles, Éditions du Jeune Barreau, 1986, pp. 345-448.

(15) Sur le régime juridique du paiement par carte, on peut consulter, notamment, X. THUNIS et M. SCHAUSS, *Aspects juridiques du paiement par carte*, précité; J.-P. BUYLE, « La carte de paiement électronique », précité.

(16) *J.O.C.E.*, n° L 208 du 2 août 1997, pp. 52-58. Pour un commentaire de ce texte, voy. M. VAN HUFFEL, « Moyens de paiement et protection du consommateur en droit communautaire et en droit belge (1re partie) », *D.C.C.R.*, n° 46, 2000, pp. 5 et s., spéc. pp. 15 et s. Cette Recommandation modifie et complète la Recommandation 88/590/CEE du 17 novembre 1988 concernant les systèmes de paiement et en particulier les relations entre les titulaires et les émetteurs de carte, *J.O.C.E.*, n° L 317 du 24 novembre 1988, p. 55.

En Belgique, un projet de loi est en préparation au ministère des Affaires économiques, qui vise à transposer en droit belge le contenu de cette recommandation (17). Des lois particulières contiennent aussi l'une ou l'autre dispositions relatives au paiement par carte : en particulier, l'article 81 de la loi du 14 juillet 1991 sur les pratiques du commerce et sur l'information et la protection du consommateur (L.P.C.) et l'article 61 de la loi du 12 juin 1991 relative au crédit à la consommation.

Pour le reste, le paiement par carte est soumis au droit commun des obligations (notamment aux règles de preuve) et des contrats. On ne saurait trop insister sur l'importance des contrats en la matière. Le droit des cartes de paiement s'est élaboré principalement par voie contractuelle. Aussi n'est-il pas exagéré d'affirmer que ce sont surtout des dispositions d'origine contractuelle — respectueuses, au demeurant, des exigences de la recommandation précitée — qui, en réalité, fixent les conditions d'utilisation des moyens de paiement par carte. De même, l'*e-banking* est régi de manière largement conventionnelle, les banques proposant généralement deux types de contrats, selon que le cocontractant soit un commerçant ou un particulier.

III. — RISQUES ET RESPONSABILITÉS

Il s'agit à présent d'identifier plus précisément les risques et responsabilités liés au paiement par WAP. A cet effet, on se propose d'organiser la réflexion autour de quatre questions clés qui seront commentées assez librement : la perte ou le vol (A), l'inexécution ou l'exécution incorrecte de l'ordre de paiement (B), le retard dans l'exécution (C) et enfin la fraude (D).

A. — *Perte ou vol*

Le dispositif technique permettant de déclencher le paiement peut être perdu ou volé : soit le GSM lui-même, avec

(17) Projet de loi relatif aux opérations effectuées au moyen d'instruments électroniques de transfert de fonds.

l'application bancaire incorporée (solution préconisée en Belgique), soit la carte à puce (solution française).

Sur ce point, les solutions à retenir ne diffèrent pas significativement de celles en vigueur en matière de cartes de paiement. A cet égard, la Recommandation de la Commission européenne du 30 juillet 1997, à laquelle se conforment largement les contrats proposés par les banques, oblige le titulaire à notifier à l'émetteur (ou à l'entité indiquée par celui-ci), dès qu'il en a connaissance, la perte ou le vol de l'instrument de paiement électronique ou des moyens qui en permettent l'utilisation (18).

Jusqu'à cette notification, le titulaire est responsable des pertes consécutives à la perte ou au vol du moyen de paiement électronique, qu'il ait ou non commis une faute ayant conduit à la perte ou au vol. Cette responsabilité est toutefois plafonnée en ce sens qu'elle ne peut dépasser 150 écus (ou euros, soit environ 6.000 FB), sauf si le titulaire a agi frauduleusement ou avec une négligence extrême, par exemple en notant son numéro d'identification personnel sous une forme aisément reconnaissable, notamment sur l'instrument de paiement lui-même ou sur un objet qu'il conserve avec cet instrument (sur le GSM; sur la carte; sur un carnet ou dans un agenda qui se trouve, avec le GSM, dans un sac à main...). Il est très important de pouvoir rapporter la preuve du moment précis de la déclaration de perte ou vol (enregistrement de la conversation téléphonique par les soins de CARD STOP, déclaration immédiate à la police...) (19). A titre d'indication, en matière de cartes, la jurisprudence, tout comme les avis de l'Ombudsman, présument la négligence grave du titulaire chaque fois qu'il ressort de la bande journal de la banque que les transactions

(18) Voir aussi, en particulier, l'article 81 de la loi du 14 juillet 1991 sur les pratiques du commerce et sur l'information et la protection du consommateur.

(19) L'article 7, § 2, litt. d), prévoit l'obligation pour l'émetteur d'assurer que des moyens appropriés soient à la disposition du titulaire pour effectuer la notification prévue à l'art. 5, b). En vertu de la même disposition, lorsque la notification est faite par téléphone, il appartient à l'émetteur (ou à l'entité spécifiée par lui) de fournir au titulaire les moyens de preuve qu'il a effectué une telle notification. L'article 7, § 2, litt. e), prévoit que l'émetteur, dans tout différend avec le titulaire, doit apporter la preuve que l'opération a été correctement enregistrée et comptabilisée, et qu'elle n'a pas été affectée par un incident technique ou une autre défaillance.

se sont réalisées sans incident et sans hésitation (ce qui donne à penser que les voleurs connaissaient le code secret).

Après notification, le titulaire n'est plus responsable des pertes consécutives à la perte ou au vol de son instrument de paiement électronique, sauf s'il a agi frauduleusement.

La solution préconisée en Belgique pour les besoins du *m-commerce* présente à cet égard un risque supplémentaire. Étant donné que les applications bancaires et outils de cryptage sont incorporés à la carte à puce SIM intégrée au GSM, le porteur doit songer à faire opposition, non seulement auprès de son opérateur de télécommunications, mais également auprès de sa banque (20).

Si le GSM est perdu ou volé, le porteur doit rapidement faire opposition (il n'est alors plus question pour lui de réaliser des achats ou de donner des ordres de paiement à l'aide de son GSM), mais, en principe, il devrait pouvoir continuer à se servir de ses cartes de crédit (utilisées en combinaison avec un autre code confidentiel).

On peut s'interroger sur le sort du portable si une des cartes de crédit est perdue ou volée : dès l'instant où le titulaire fait opposition, tout le GSM sera-t-il bloqué (*i.e.* toutes les cartes de crédit liées à la clé privée du porteur) ou seulement la carte de crédit perdue ou volée? Cette dernière solution paraît plus fine, mais il reste à savoir si elle peut être gérée pratiquement. A moins d'estimer que le GSM ne doit être bloqué en aucune de ses applications bancaires, ce qui serait idéal. La solution retenue dépend de savoir si l'on privilégie en définitive une conception physique ou virtuelle de la carte de crédit. Au moment où ces lignes sont écrites, il est encore trop tôt pour se prononcer sur ce point.

En marge du problème de l'opposition, un mot doit être dit de l'utilisation du mécanisme de signature électronique. On enseigne habituellement que le risque de fraude le plus vraisemblable — quoique faible — en matière de signature est lié à la perte de maîtrise de la clé privée par son titulaire. Ici ce risque peut être écarté, semble-t-il. La clé privée est logée dans

(20) En France, par contre, le GSM est « anonyme » du point de vue bancaire puisque l'application bancaire est intégrée dans la carte bleue qui est une pièce distincte et indépendante du portable WAP.

une zone protégée de la carte SIM et, d'un point de vue technique, elle est en principe inaccessible à la lecture par un tiers (au cours d'une connexion). En outre, le code *Banking-PIN* est vérifié à l'intérieur de l'application — comme, du reste, dans l'hypothèse où le GSM serait doté d'un lecteur de carte à mémoire — et ne circule évidemment pas sur le réseau. Dès lors, on ne voit pas d'hypothèse sérieuse où le porteur devrait faire diligence pour obtenir la révocation du certificat contenant sa clé publique.

B. — *Inexécution ou exécution incorrecte de l'ordre*

L'hypothèse est que le titulaire du GSM donne un ordre de paiement à sa banque et que celui-ci n'est pas exécuté. La responsabilité incombe, en principe, à la banque pour manquement à son obligation — de résultat — d'effectuer l'opération prévue dans le cadre des conditions contractuelles (21).

C'est ce que prévoit la recommandation de 1997, en son article 8 : « *l'émetteur est responsable de l'inexécution ou de l'exécution incorrecte des opérations [dont il est chargé]* », telles que les transferts de fonds effectués au moyen d'un instrument de paiement électronique. Cette responsabilité est étroitement limitée puisque l'indemnisation due est plafonnée à une somme égale au montant de l'opération non exécutée ou incorrectement exécutée, éventuellement augmentée de dommages et intérêts. Cette responsabilité peut ne pas suffire à réparer les conséquences dommageables de la non exécution qui seront mises à charge du client par son fournisseur impayé. Dans certains cas, en effet, la date du paiement joue un rôle important et un retard de paiement peut être particulièrement dommageable (22).

C — *Retard dans l'exécution*

Le dommage subi par le client suite à un retard dans l'exécution d'un ordre de paiement doit logiquement être réparé par la banque. En son article 8, § 3, la recommandation de

(21) En ce sens, *mutatis mutandis*, J. HUET, *op. cit.*, p. 290, n° 8, *a*).
(22) Sur le problème du moment du paiement, voy. la contribution de INGBER.

1997 dispose que « *toutes les autres conséquences financières éventuelles, liées en particulier à la détermination de l'étendue du dommage indemnisable, sont à la charge de l'émetteur (...)* ».

A cet égard, dans un contrat de *home banking* examiné, on trouve la clause d'exonération de responsabilité reproduite ici (que l'on retrouvera aussi vraisemblablement dans les conditions générales appelées à régir le *m-banking*), en l'occurrence une clause extensive de force majeure complétée par une limitation de réparation : « *La banque apporte les meilleurs soins au bon fonctionnement du service et s'engage à donner aussi rapidement que possible la suite appropriée aux ordres reçus. La banque ne peut être rendue responsable des interruptions ou retards dus aux pannes techniques, à la force majeure, au fait de tiers ou à toutes circonstances, quelles qu'elles soient, indépendantes de sa volonté. Au cas où sa responsabilité serait tout de même retenue, la banque ne sera en aucune façon redevable d'une quelconque indemnité pour dommage immatériel ou indirect tel que préjudice commercial ou d'exploitation, perte de bénéfice, etc.* »

Et, dans un contrat de *web banking*, on trouve la clause suivante : « *La banque n'accepte aucune responsabilité relative aux conséquences directes ou indirectes d'un mauvais fonctionnement de l'équipement du client ou du service public de télécommunications ou en cas d'interruption du service consécutive à des circonstances indépendantes de sa volonté. Ceci vaut également pour la destruction ou l'endommagement de fichiers ou de tout autre document ou information stocké sur les ordinateurs du client ainsi que pendant et après une intervention de la banque sur ce matériel. Le client doit veiller à mettre ces informations en sécurité* ».

Cette clause paraît raisonnable : on admet d'ordinaire que les interruptions d'électricité et le mauvais fonctionnement des réseaux de télécommunication constituent (ici pour la banque) un fait répondant aux conditions de la cause étrangère exonératoire. Cela pose le problème des recours, assez aléatoires, des clients contre les opérateurs de réseau. Seront plus particulièrement intéressés à exercer un tel recours les banques ou les sociétés commerciales, qui peuvent subir un préjudice important par suite de lignes encombrées, transmissions lentes et problèmes de débit.

D'emblée, il faut remarquer que cette hypothèse est étrangère au régime d'exonération de responsabilité institué au profit des opérateurs de réseau par les articles 12 et 15 combinés de la directive européenne du 8 juin 2000 sur le commerce électronique (23). L'exonération concerne les informations émanant de tiers et transmises à des tiers. Or ici, c'est, non le contenu véhiculé, mais le service de communication lui-même qui est en cause. La responsabilité de l'opérateur téléphonique défaillant peut théoriquement être recherchée sur la base du droit commun (art. 1382 C. civ.). C'est ce qui ressort du nouvel et curieux article 105*decies* B de la loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques, article inséré par la loi du 19 décembre 1997 (art. 66) et remplaçant l'ancien article 64 qui établissait un régime de responsabilité limitée — ou, si l'on préfère, d'immunité tempérée — pour Belgacom. L'article 105*decies* B dispose que « *[l]e Roi peut, par arrêté délibéré en Conseil des ministres, sur proposition de l'Institut et après avis du Comité consultatif, modifier la responsabilité qui incombe aux opérateurs de réseaux publics de télécommunications et aux opérateurs de services de téléphonie vocale du chef du non-fonctionnement ou du fonctionnement défectueux du réseau public de télécommunications ou du chef de manquements dans la fourniture du service de téléphonie vocale* ».

Manifestement, le législateur n'indique pas dans quel sens il souhaite voir modifier le régime de responsabilité. D'après nos informations, cette disposition est interprétée diversement. Certains y voient un relent de la notion de service public : dans cette optique, le Roi pourrait instaurer certaines limites de responsabilité au bénéfice des opérateurs de réseau. D'autres y voient la possibilité pour le Roi de limiter le recours aux clauses d'exonération de responsabilité. Quoi qu'il en soit, en attendant, les recours introduits contre les opérateurs de réseau se heurteront aux clauses restrictives de responsabilité stipulées par ces derniers (24).

(23) Directive 2000/32/CE du Parlement européen et du Conseil du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur (« directive sur le commerce électronique »), *J.O.C.E.*, L 188/1 du 17 juillet 2000.

D. *Fraude*

Tout porte à croire que le risque de fraude peut être ici minimisé.

En matière de paiement, les fraudes possibles ont pour nom fabrication de fausse carte, forçage du dispositif de sécurité et introduction/maintien frauduleux dans un système de traitement de données, en l'occurrence, au niveau de la banque ou sur le site WAP de cette dernière. Ce type de fraude fait désormais l'objet d'incriminations pénales spécifiques définies dans la loi sur la criminalité informatique approuvée récemment par le Parlement (25).

Dans la solution mise au point en Belgique, en cas de fraude réalisée au moyen d'une fausse carte, on est renvoyé à la question de savoir si tout le GSM se trouve bloqué ou seulement la carte qui a fait l'objet d'une falsification. La « carte à puce »

(24) Dans les conditions générales d'un opérateur de mobilophonie (désigné par XXX), on peut épingler la clause suivante : « *XXX s'engage à mettre en œuvre tous les moyens afin d'assurer le bon fonctionnement de ses Services. XXX détermine de quelle manière les moyens techniques optimaux sont mis en œuvre. XXX souhaite, toutefois, attirer l'attention du client sur le fait qu'une transmission parfaite ne peut pas toujours être garantie, car les signaux radio peuvent être entravés par des facteurs externes tels les immeubles, la végétation ou le relief.*

La qualité des Services XXX peut être également influencée par le type de téléphone mobile utilisé. XXX attire l'attention du client qui l'accepte, sur le fait qu'il ne peut bénéficier pleinement des Services XXX que s'il dispose d'un téléphone mobile 'dual band' adapté à la technologie du réseau XXX. C'est ainsi que le GSM XXX et le Téléphone Mobile Agréé par XXX ont été spécifiquement conçus pour les Services XXX. Le client a été spécifiquement informé qu'il ne peut pas, ou seulement dans une mesure très limitée, utiliser des Services XXX s'il utilise un téléphone mobile GSM 900.

XXX décline toute responsabilité en cas de dérangement ou de défaut de qualité imputable à des facteurs externes, sans préjudice, toutefois, de la garantie de fabrication standard liée au GSM XXX et au Téléphone Mobile Agréé par XXX. XXX décline également toute responsabilité pour les dérangements éventuels causés à la suite de travaux d'entretien, d'amélioration ou d'extension des installations.

XXX prend toutes les mesures raisonnables afin d'assurer la sécurité et la fiabilité du réseau XXX. XXX décline toute responsabilité pour les dommages qui, malgré ces mesures, sont causés par un tiers. Ainsi, XXX n'est pas responsable en cas d'écoute d'une communication par un tiers ».

(25) Consultez, sur le site web de la Chambre des Représentants, les dossiers n^{os} 213 et 214.

à la française (carte bleue), elle, est jugée difficile à falsifier, même si l'on sait à présent que le risque n'est pas nul (26)!

Le risque est évidemment plus ou moins grand selon le système de sécurité mis en place. En principe, c'est à la banque d'assumer le risque de fraude car elle est dépositaire des fonds des clients et doit les restituer (27). En ce sens, la recommandation de 1997 précise que l'émetteur est responsable des opérations effectuées sans autorisation du titulaire, et de toute erreur ou irrégularité commise dans la gestion de son compte et imputable à l'émetteur. Sa responsabilité porte sur la somme nécessaire pour rétablir le titulaire dans la situation où il se trouvait avant l'opération non autorisée. Pour échapper à sa responsabilité, il revient à la banque de démontrer une éventuelle faute du client, par exemple dans la conservation de son code... qu'il aurait laissé traîner sur un papier ou dans un agenda à proximité de son GSM, lui-même plus ou moins égaré...

Cela étant, dans un contrat de *web banking*, on trouve la clause ici reproduite (qui pourrait bien apparaître aussi dans les conditions générales gouvernant le *m-banking*) : « *Hormis en cas de faute grave et intentionnelle de la banque, toute conséquence directe ou indirecte d'une utilisation erronée, frauduleuse ou abusive du service de* net banking, *que ce soit de la part du client ou de la part de tiers, ne sera en aucun cas imputable à la banque* ». On se demande comment un juge apprécierait cette exonération, spécialement en ce qu'elle couvre le cas d'une utilisation erronée, frauduleuse ou abusive de la part de tiers.

Toujours sur le terrain de la fraude, on relève qu'à la différence de l'*e-commerce*, où parfois le télépaiement s'opère moyennant la simple communication du numéro apparent de la carte de crédit (et souvent de la date d'expiration), avec le risque d'interception que comporte cette pratique douteuse, en matière de paiement par WAP, le numéro de la carte de crédit ne transite sur le réseau dans aucune des solutions préconisées.

(26) Cf. l'affaire « Humpich » du nom de l'informaticien qui, de son propre aveu, aurait percé l'algorithme de la Carte Bleue française, T.G.I. Paris (13e ch. corr.), 25 février 2000 (le jugement est disponible sur le web à l'url www.legalis.net).

(27) A ce sujet, X. THUNIS, *op. cit.*, pp. 247 et s.

En définitive, la fraude devrait être, théoriquement, une hypothèse d'école. On peut se demander dès lors si les banques ne pourraient pas souscrire une obligation de garantie liée au dispositif de sécurité mis en œuvre. La banque garantirait qu'aucune opération ne pourra être effectuée sur le compte du client sans l'intermédiaire du dispositif de sécurité visé (carte à puce hautement sécurisée ou carte SIM « enrichie » selon la solution Banksys).

OBSERVATIONS FINALES

Au seuil de notre réflexion, nous évoquions ce reproche souvent adressé au droit d'être à la remorque des faits, et spécialement, des avancées technologiques. Mais, indépendamment de savoir s'il pourrait en être autrement, n'est-il pas généralement souhaitable que la vie précède la norme ? Toujours est-il que notre tour d'horizon des questions de responsabilité liées au paiement par WAP ne plonge pas le juriste dans un abîme de perplexité.

Bien sûr, notre recherche demeure forcément fragmentaire et invite donc à la prudence. Mais, enfin, tout porte à croire que, une fois la nouveauté assimilée, on peut se tourner vers un certain nombre de principes et règles de droit commun, bien établis et familiers. D'autant que ladite nouveauté est désormais toute relative dans la mesure où le paiement par WAP, quel qu'en soit le type, n'est jamais qu'une forme de télépaiment. Or ce dernier, lui aussi, a déjà fait l'objet de quelques règles spécifiques, peu nombreuses à vrai dire, issues de la jurisprudence et du législateur, sans compter la Recommandation de la Commission européenne du 30 juillet 1997 « concernant les opérations effectuées au moyen d'instruments de paiement électronique, en particulier la relation entre émetteur et titulaire ».

Pour le reste, on l'a vu, la matière est régie surtout par voie conventionnelle. Cette méthode présente quelque difficulté. En effet, s'il est aisé de mettre la main sur les conditions générales relatives aux services offerts aux clients des banques, les conventions inter-bancaires ou celles conclues entre les banques et leur filiale commune Banksys sont, elles, largement

confidentielles. Mais, ici encore, rien de propre au paiement par WAP.

Le développement et la généralisation de ce nouveau moyen de communication et de paiement dépendront fortement du degré de confiance que les utilisateurs placeront en lui. A cet égard, le point névralgique est certainement la sécurité des procédés offerts, en termes de protection contre les fraudes, sous leurs diverses formes, et de confidentialité des opérations. Le grand défi se situe dès lors du côté de la fiabilité des dispositifs de sécurité mis en place et des outils de cryptographie disponibles.